+44 345 094 0945
www.waterstons.com

News article

Jul 2024

Fight cyber-threats from the outset: Inside Small Business

Why start-ups must prioritise cyber-security and get comfortable with the fundamentals.

In today's digital landscape, where technology reigns supreme, cyber-threats loom large for organisations across all sectors. While large corporations often invest heavily in cyber-security defences, it is disheartening to observe that many start-ups overlook the importance of safeguarding their digital assets. Throughout my 20-plus-year career, I've seen first-hand that start-ups are not immune to cyberattacks and I cannot emphasise enough how critical it is to prioritise security from the start. Neglecting this aspect can be a fundamental and costly mistake with severe consequences.



Charlie Hales, Managing Director, Waterstons Australia

The rise of start-ups and cyberattacks

Start-ups, with their innovation, agility and potential for disruptive growth, have become a driving force in the modern economy; however, their rapid rise also makes them attractive targets for cyber-criminals and other bad actors. Start-ups, by nature, often possess valuable intellectual property, sensitive customer data and innovative ideas, making them prime targets for data breaches, intellectual property theft, and other malicious activities.

Why start-ups neglect security

Despite the clear and present danger cyberattacks pose, many start-ups tend to overlook security in the early stages. Several reasons contribute to this short-sightedness:

- **Not understanding your data:** In the dynamic world of business, comprehending your data is paramount. Without a deep understanding of the information you possess, the intellectual property you safeguard, and the necessary levels of confidentiality, true cyber protection remains elusive. Once this understanding is attained, however, it becomes the basis for weaving a tapestry of cyber-security and controls that fortify your business and extend to trusted third parties.
- **Lack of resources:** Start-ups, particularly in their nascent stages, often operate with limited resources. Budget constraints and competing priorities force them to make difficult decisions. Unfortunately, security is frequently deprioritised due to perceived high costs or an underestimation of the potential risks involved.
- **Overemphasis on growth:** Start-ups are under immense pressure to build their user base rapidly, acquire investors and secure funding. This growth-centric mindset often leads them to allocate resources primarily towards product development, marketing and customer acquisition, inadvertently neglecting security measures.
- **Misconceptions about vulnerability:** Some start-ups mistakenly believe they are not attractive targets for cyber-criminals due to their small size or relative anonymity. But attackers are indiscriminate and often exploit any vulnerabilities they encounter. Neglecting security based on false assumptions can prove disastrous.

Consequences of neglecting security

The consequences of overlooking security in the early stages can be severe and far-reaching for start-ups:

- **Loss of Intellectual Property:** Start-ups rely heavily on their innovative ideas and intellectual property for a competitive edge. A successful cyberattack can result in the theft of proprietary information, undermining the very foundation of a start-up's business model.
- **Damaged reputation:** Start-ups build their reputation on trust and credibility. A breach that compromises customer data can shatter that trust, leading to reputational damage that is difficult to repair. Such incidents can also lead to legal liabilities and regulatory penalties. Some businesses never recover their reputation.
- **Financial impact:** Recovering from a cyberattack can be financially crippling for start-ups. The costs associated with incident response, legal expenses, possible customer compensation and infrastructure repairs can drain limited resources and even threaten the survival and long-term viability of the business.

Prioritising security from the start

Start-ups must recognise that cyber-security is not an afterthought, nor something best sorted out down the track when the business is profitable; it is an essential investment in their long-term success. Here are some key steps that start-ups should take to prioritise security:

- **Create a security culture:** Establish a security-first mindset across the organisation. Educate employees about best practices, implement security policies, and ensure that security is ingrained in every aspect of the start-up's operations. As everyone within an organisation is a potential cyber vulnerability, cyber security is everyone's business.
- **Implement robust security measures:** Deploy a multi-layered security framework that includes firewalls, intrusion detection systems, strong authentication protocols, regular software updates, and encryption. Employing security technologies and tools can help prevent and mitigate cyberattacks.
- **Conduct regular audits and assessments:** Perform routine security audits and vulnerability assessments to identify weaknesses and address them proactively. Engage with cyber-security experts early to conduct penetration testing and ensure that your security is robust.

IT personnel play a crucial role in the success of most start-ups. Some IT specialists may have a general understanding of security concepts, but their expertise usually lies more in managing and maintaining IT infrastructure that is specific to the business, its role and function. Whereas cyber-security specialists possess in-depth knowledge of various security frameworks, industry best practices, compliance regulations and emerging threats. They stay up to date with the latest security vulnerabilities and attack vectors, understanding how to mitigate risks and protect sensitive information.

These distinctions are not absolute, and there may be individuals who possess a blend of IT and cyber-security skills, but in our experience, having IT work with cyber experts provides the best solutions and protections.

Unfortunately, it has happened in start-ups where progress is halted in the first year due to a cyber incident. As discussed above, start-ups need to build a great reputation to Tsupport their growth and putting your cyber practice foundations in place early can protect you from failing due to an incident that could have been easily avoided.

A case study

Failing to prioritise good cyber posture from day one can be a severe mistake. One start-up's leaders believed they were unlikely to be targeted by cyber-threats and found out they were wrong in a devastating way.

The finance director's (FD) emails were breached by a hacker. Seizing the opportunity, the hacker intercepted invoicing emails from a major third-party company. Then, posing as the legitimate third party, the hacker sent an email from the actual invoice thread, requesting that the FD change the payment bank details. Unfortunately, the FD fell victim to this deception, assuming it was a legitimate request, and made the payment to the hacker's account.

This went undetected for a few weeks, until the real third party began seeking payment for the true invoice. It was only then that the start-up realised it had fallen victim to a cyberattack and was left financially exposed.

With no insurance or cyber plans in place, the start-up was left unable to file a claim and recover the lost funds. This unfortunate incident served as a harsh lesson that good cyber hygiene is critical to a business, which is when the start-up got in touch with us.

We worked with the business's leaders to improve its overall cyber posture, ensuring that it's in a much better position now. Our work included phishing simulations, user education and instilling a great cyber culture designed to address the previous issues directly. While the company now has comprehensive cyber controls in place to deal with the overall threat landscape, this experience highlights the speed at which a business can suddenly be exposed to a cyber threat, and the importance of implementing well-designed cyber security protocols, including insurance.

PQ: Neglecting security based on false assumptions can prove disastrous.

Thanks for partnering with us on this article, Fight cyber-threats from the outset - Inside Small Business